The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/14/2016

SUBJECT:
Multiple Vulnerabilities in Joomla Could Allow for Arbitrary File Upload

OVERVIEW:
Multiple vulnerabilities have been discovered in Joomla, the most severe of which could allow for arbitrary file upload that may lead to arbitrary code execution. Joomla is an open source content management system for websites. Successful exploitation of these vulnerabilities could allow an attacker to upload arbitrary files to the affected computer that may result in arbitrary code execution, elevation of privilege, or information disclosure.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Joomla versions 1.6.0 through 3.6.4

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Joomla! Core, the most severe of which allow for arbitrary file upload that may lead to arbitrary code execution. Details of the vulnerabilities are as follows:

- One Arbitrary File Upload vulnerability exists due to inadequate filesystem checks allowing files with alternative PHP file extensions to be uploaded. (CVE-2016-9836)
- One Information Disclosure vulnerability exists due to inadequate ACL checks in the Beez3 com_content article layout override enables a user to view restricted content. (CVE-2016-9837)

- One Elevation of Privilege vulnerability exists due to incorrect use of unfiltered data stored to the session on a form validation failure allows for existing user accounts to be modified; to include resetting their username, password, and user group assignments. (CVE-2016-9838)

Successful exploitation of these vulnerabilities could allow an attacker to upload arbitrary files to the affected computer that may result in arbitrary code execution, elevation of privilege, or information disclosure.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Joomla! to vulnerable systems immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Joomla!:

https://developer.joomla.org/security-centre.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9836
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9837
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9838